

Gordon Rees Scully Mansukhani LLP
300 S. 4th Street, Suite 1550
Las Vegas, Nevada 89101

ROBERT E. SCHUMACHER, ESQ.

Nevada Bar No. 7504

GORDON REES SCULLY MANSUKHANI, LLP

300 S. 4th Street, Suite 1550

Las Vegas, NV 89101

Telephone: (702) 577-9300

Direct Line: (702) 577-9319

Facsimile: (702) 255-2858

Email: rschumacher@grsm.com

AND

THOMAS H. CELLILLI III, ESQ.

(Pro Hac Vice Forthcoming)

SKARZYNSKI MARICK & BLACK, LLP

One Battery Park Plaza, 32nd Floor

New York, NY 10004

Telephone: (212) 820-7700

Direct Line: (212) 820-7736

Facsimile: (212) 820-7740

Email: tcellilli@skarzynski.com

Attorneys for Tokio Marine Houston Casualty Company

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

Tokio Marine Houston Casualty Company,
a foreign Corporation,

Plaintiff

vs.

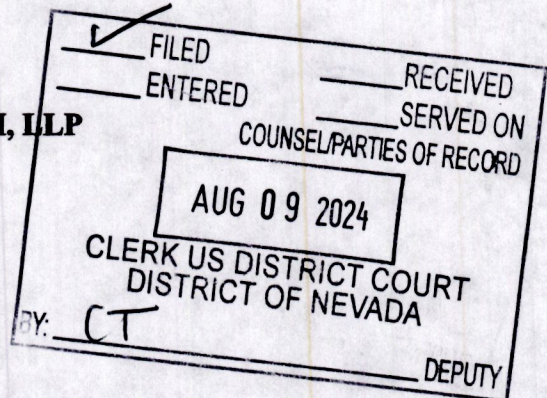
Findlay Management Group., a Nevada
Domestic Corporation,

Defendant.

CASE NO. 2:24-cv-01459 - *GMN-NJK*

**DECLARATORY JUDGMENT
COMPLAINT AND DEMAND FOR
JURY TRIAL**

The Plaintiff, TOKIO MARINE HOUSTON CASUALTY COMPANY (hereinafter
"Tokio Marine HCC"), a foreign corporation, by and through its attorneys, brings this
Declaratory Judgment Complaint and Demand for Jury Trial against Defendant Findlay



Gordon Rees Scully Mansukhani LLP
300 S. 4th Street, Suite 1550
Las Vegas, Nevada 89101

1 Management Group (hereinafter "Findlay"), and hereby alleges as follows:

2 **INTRODUCTION**

3 1. Findlay owns and operates automotive dealerships in and across Nevada, Arizona,
4 Utah & Idaho. At approximately 8:00 a.m. PDT on June 7, 2024, Findlay discovered a
5 ransomware attack encrypting its computer network (hereinafter "Ransomware Attack").

6 2. At the time of the Ransomware Attack, Findlay was without cyber insurance
7 coverage as its cyber policy with Tokio Marine HCC, which was in effect from June 1, 2023, to
8 June 1, 2024 (the "2023/24 Policy"), expired on June 1, 2024 at 12:01 a.m. PDT.

9 3. With full knowledge of the Ransomware Attack and that it was without cyber
10 coverage when discovering the Ransomware Attack, Findlay and its agents sought to renew the
11 expired cyber insurance policy for a new policy to begin June 1, 2024 to June 1, 2025 (the
12 "2024/25 Prospective Policy") by, among other means, submitting a backdated application which
13 contained material omissions and misrepresentations in an effort to conceal the Ransomware
14 Attack to fraudulently induce Tokio Marine HCC into binding and issuing a cyber insurance
15 policy.
16

17 4. On June 7, 2024, at 9:42 a.m. after discovering the Ransomware Attack, Findlay,
18 through its retained agent Thaxton & Associates ("Thaxton"), requested that Tokio Marine HCC
19 bind coverage, effective June 1, 2024, and that it would coordinate the signed required binding
20 documents as soon as possible.

21 5. Between June 7, 2024 when learning of the Ransomware Attack and continuing
22 through June 10, 2024 when it notified Tokio Marine HCC of the Ransomware Attack, Findlay
23 made material omissions and misrepresentations with the sole intent of inducing Tokio Marine
24 HCC to bind and issue a cyber policy in the known absence of coverage.

25 6. Pursuant to 28 U.S.C. §1332, Tokio Marine HCC brings this Declaratory
26 Judgment Complaint and Demand for Jury Trial against Findlay.

27 7. Tokio Marine HCC seeks a declaration that no policy of insurance exists between
28 it and Findlay as neither a binder nor policy was ever delivered to Findlay once Tokio Marine

Gordon Rees Scully Mansukhani LLP
300 S. 4th Street, Suite 1550
Las Vegas, Nevada 89101

1 HCC became aware of Findlay's fraudulent conduct.

2 8. Tokio Marine HCC seeks a declaration that if it is determined that a binder was
3 delivered for the 2024/25 Prospective Policy, the binder is rescinded and declared null and *void*
4 *ab initio* because of material omissions and misrepresentations of Findlay to fraudulently induce
5 Tokio Marine HCC into issuing the binder.

6 9. Tokio Marine HCC seeks a declaration that it is not obligated to pay for any
7 losses arising out of the Ransomware Attack or defend or indemnify Findlay for any class action
8 suits or other third party liabilities arising out of the Ransomware Attack.

9 NATURE OF ACTION

10 10. This is an action for declaratory relief under 28 U.S.C. §2201 regarding a dispute
11 concerning coverage obligations involving a potential cyber liability insurance policy and the
12 parties' respective rights, duties, and obligations flowing therefrom.

13 JURISDICTION AND VENUE

14 11. The litigation is a civil action over which this Court has original diversity
15 jurisdiction pursuant to 28 U.S.C. §1332.

16 12. The amount in controversy in this matter exceeds \$75,000.

17 13. Findlay resides and conducts business in this District. A substantial part of the
18 actions giving rise to the claim also occurred in this District. Therefore, venue is proper in this
19 District pursuant to 28 U.S.C. §1391.

20 PARTIES

21 14. Tokio Marine Houston Casualty Company is a Texas corporation with its
22 principal place of business in the State of Texas, and is duly licensed to conduct business in
23 Nevada.

24 15. Findlay Management Group is a Nevada domestic corporation with its principal
25 place of business located in the State of Nevada.

26 BACKGROUND FACTS

27 16. Tokio Marine HCC issued Netguard® Plus Cyber Liability Insurance Policy No.

Gordon Rees Scully Mansukhani LLP
300 S. 4th Street, Suite 1550
Las Vegas, Nevada 89101

1 H23NGP216991-01 ("2023/24 Policy") to Findlay for Claims first made and Events first
2 discovered from June 01, 2023 to June 01, 2024. The Maximum Policy Aggregate Limit of
3 Liability was \$5,000,000. The 2023/24 Policy expired on June 1, 2024 at 12:01 a.m. local time in
4 Henderson, Nevada (PDT).

5 17. At no time before or after the 2023/24 Policy expired, did Findlay seek to extend
6 the 2023/24 Policy nor did Tokio Marine HCC grant permission to do so.

7 18. Negotiations for a renewal policy for the June 1, 2024 to June 1, 2025 policy year
8 began between Tokio Marine HCC and Findlay and its agents, including Thaxton, as early as
9 mid-April 2024.

10 19. On May 8, 2024, Findlay submitted to Tokio Marine HCC a renewal insurance
11 application signed by John Steffy, CIO and dated April 30, 2024 for Netguard® Plus Cyber
12 Liability Insurance (**Exhibit 1**). Tokio Marine HCC, through wholesale broker CRC, advised
13 Findlay's representative Thaxton, that pre-binding subjectivities remained open. Findlay and
14 Thaxton were directly advised as early as June 4, 2024 that Findlay was "bare" and without any
15 cyber insurance policy coverage after June 1, 2024.

16 20. Findlay, through its agent Thaxton, continued to negotiate a reduced premium for
17 a prospective policy through June 5, 2024.

18 21. On June 7, 2024, at 9:42 a.m. PDT, Thaxton emailed CRC requesting that the
19 wholesale broker CRC "[p]lease bind coverage effective 6/1/2024 per the attached quote. We
20 will coordinate the signed required binding documents as soon as possible." (**Exhibit 2**). At the
21 time of this request, Findlay and its agents were aware of the Ransomware Attack. Findlay
22 discovered the Ransomware Attack at approximately 8:00 a.m. PDT and had advised Thaxton of
23 the same at approximately 9:00 a.m. PDT on June 7, 2024.

24 22. Thereafter, on June 7, 2024 and continuing through Monday, June 10, 2024,
25 Thaxton telephoned and corresponded with CRC and Tokio Marine HCC regarding the required
26 pre-binding subjectivities, including the requirement that a re-signed application be submitted,
27 and that Findlay answer questions pertinent to the use of a CiscoASA VPN. These exchanges
28

Gordon Rees Scully Mansukhani LLP
300 S. 4th Street, Suite 1550
Las Vegas, Nevada 89101

1 occurred from June 7, 2024 through Monday, June 10, 2024 without Findlay or Thaxton ever
2 advising Tokio Marine HCC or CRC of the June 7th Ransomware Attack.

3 23. On June 7, 2024, at 10:30 a.m. PDT, the application for insurance coverage was
4 re-signed by Mr. Tyler Corder, Findlay's CFO, and submitted to Tokio Marine HCC.

5 24. The application signed on April 30, 2024 by CIO, John Steffy and the application
6 re-signed on June 7, 2024 at 10:30 a.m. PDT by CFO Tyler Corder, state as follows at the
7 Certification and Signature section:

8 It is further agreed that, if in the time between submission of this
9 application and the requested date for coverage to be effective, the
10 Applicant becomes aware of any information which would change
11 the answers furnished in response to any question of this
12 application, such information shall be revealed immediately in
writing to the Underwriter.

13 25. Section 10 of the Application is entitled "LOSS History", and asks the applicant
14 in pertinent part as follows:

15 a. In the past 3 years, has the Applicant or any other person or
16 organization proposed for this insurance:

17 ...

(4) Received any cyber extortion demand or threat?

(5) Sustained any unscheduled network outage or interruption
18 for any reason?

19 ...

20 b. Do you or any other person or organization proposed for this
21 insurance have knowledge of any security breach, privacy-
related event or incident or allegations of breach of privacy that
22 may give rise to a claim?"

23 26. Mr. Corder responded "No" to these questions on behalf of Findlay. (**Exhibit 3**)

24 27. On June 10, 2024, at 11:24 a.m. PDT, based solely on communications from
25 Findlay and its agent Thaxton, Tokio Marine HCC created a "bind" document that was shared
26 with CRC, the wholesale broker. However, upon discovering this timeline of concealment,
27 misrepresentation, and fraud, Tokio Marine HCC did not issue or deliver the binder to Findlay or
28 Thaxton.

28 28. On June 10, 2024, at 3:05 p.m. PDT, Findlay notified Tokio Marine HCC and the

Gordon Rees Scully Mansukhani LLP
300 S. 4th Street, Suite 1550
Las Vegas, Nevada 89101

2024/25 Prospective Policy of the Ransomware Attack. At the time of the notification, the binder had not been issued or delivered.

29. On June 14, 2024, Findlay notified Tokio Marine HCC and the 2024/25 Prospective Policy of a class action complaint filed on June 12, 2024, by Karen Smith and Pholisith Bouphapraseuth in the Eighth Judicial District Court, Clark County, Nevada, Case No. A-24-895258-C, and removed on July 8, 2024, to the U.S. District Court for the District of Nevada, Case No. 2:24-cv-01226, resulting from the Ransomware Attack.

30. On June 21, 2024, Findlay notified Tokio Marine HCC and the 2024/25 Prospective Policy of a class action complaint filed on June 21, 2024, by Susan Stevens against Findlay in the Eighth Judicial District Court, Clark County Nevada, Case No. A-24-895977-C, and removed on July 8, 2024, to the U.S. District Court for the District of Nevada, Case No. 2:24-cv-01227, resulting from the Ransomware Attack.

31. On June 20, 2024, Findlay notified Tokio Marine HCC and the 2024/25 Prospective Policy of an outage of Findlay's Dealer Management System vendor, CDK Global, due to a cyber incident, which impacted Findlay's business operations.

FIRST CAUSE OF ACTION Declaratory Relief

32. Tokio Marine HCC repeats, reiterates and realleges each and every allegation of the preceding paragraphs of this Complaint and incorporates them by reference here.

33. Tokio Marine HCC and Findlay have a justiciable controversy concerning whether a binder of insurance coverage for the 2024/25 Prospective Policy was delivered to Findlay.

34. There exists a bona fide actual, present and practical need for a declaration regarding the existence of a binder and insurance policy for the 2024/25 Prospective Policy and the dispute between Tokio Marine HCC and Findlay is of sufficient immediacy due in part to the pendency and potential future filings of class action lawsuits against Findlay in Clark County, Nevada, to warrant the issuance of a declaratory judgment.

SECOND CAUSE OF ACTION

Rescission

39. Tokio Marine HCC justifiably relied on the representations made in Findlay's insurance application and the negotiations to obtain insurance coverage in determining whether

1 to issue the policy under the terms provided and determining the appropriate premium to be
2 charged.

3 40. If the true facts had been known, Tokio Marine HCC would not have issued a
4 binder of insurance policy and/or would not have provided coverage under the same terms or
5 with respect to the hazard resulting in the claims at issue.

6 41. Therefore, Tokio Marine HCC is entitled to a declaration that the Tokio Marine
7 HCC's binder for the 2024/25 Prospective Policy is *void ab initio* and/or rescinded .

8 PRAYER FOR RELIEF

9 WHEREFORE, Tokio Marine HCC requests judgment in its favor and against Findlay as
10 follows:

11 (a) A judicial declaration that no policy of insurance exists between Tokio Marine
12 HCC and Findlay as neither a binder nor policy was ever delivered to Findlay for the 2024/25
13 Prospective Policy;

14 (b) A judicial declaration that if it is determined that a binder was delivered for the
15 2024/25 Prospective Policy, that the binder is rescinded because of material omissions and
16 misrepresentations made by Findlay that were intended to fraudulently induce and did
17 fraudulently induce Tokio Marine HCC into issuing the binder;

18 (c) A judicial declaration that Tokio Marine HCC is not obligated to provide
19 coverage for any costs, expenses, losses, attorneys' fees, first party liabilities, or otherwise
20 relating to/arising from the Ransomware Attack;

21 (d) A judicial declaration that Tokio Marine HCC is not obligated to defend or
22 indemnify Findlay for class action suits or any other third party liabilities arising out of the
23 Ransomware Attack; and

24 (e) A judicial declaration that Tokio Marine HCC has no obligations with respect to
25 any notifications made to Tokio Marine HCC for the 2024/25 Prospective Policy, including the
26 CDK system outage.
27
28

JURY TRIAL DEMAND

Tokio Marine HCC hereby demands that this matter be tried before a jury.

DATED this 8th day of August 2024.

**GORDON REES SCULLY
MANSUKHANI, LLP**

/s/ Robert E. Schumacher

ROBERT E. SCHUMACHER, ESQ.

Nevada Bar No. 7504

300 S. 4th Street, Suite 1550

Las Vegas, NV 89101

And

**THOMAS H. CELLILLI III, ESQ. (*Pro Hac
Vice Forthcoming*)**

SKARZYNSKI MARICK & BLACK, LLP

One Battery Park Plaza, 32nd Floor

New York, NY 10004

Attorneys for Plaintiff,

Tokio Marine Houston Casualty Company

Gordon Rees Scully Mansukhani LLP
300 S. 4th Street, Suite 1550
Las Vegas, Nevada 89101

TABLE OF EXHIBITS

Exhibit	Description
1.	Netguard® Plus Cyber Liability Insurance
2.	June 7, 2024 Email from Ronda Miner
3.	Netguard® Plus Cyber Liability Insurance questionnaire

Gordon Rees Scully Mansukhani LLP
300 S. 4th Street, Suite 1550
Las Vegas, Nevada 89101

EXHIBIT 1

NETGUARD® PLUS CYBER LIABILITY INSURANCE

TOKIOMARINE
HCC

NetGuard® Plus Cyber Liability Insurance

APPLICATION

THIS IS AN APPLICATION FOR A CLAIMS MADE AND REPORTED POLICY. THIS APPLICATION IS NOT A BINDER.

This application for NetGuard® Plus Cyber Liability Insurance is intended to be used for the preliminary evaluation of a submission. When completed in its entirety, this application will enable the Underwriter to decide whether or not to authorize the binding of insurance. Please type or print clearly and answer all questions. If space is insufficient to answer any question fully, attach a separate sheet. Complete all required supplemental forms/applications. "You" and "Your", as used in this application, means the Applicant unless noted otherwise below.

Please refer to the attached Cyber Glossary for an explanation of the cyber security terms that appear in bold face type.

1. GENERAL INFORMATION

Name of Applicant: Findlay Management

Street Address: 310 N. Gibson Road

City, State, Zip: Henderson

Phone: [REDACTED]

Website: findlayauto.com

Fax: [REDACTED]

2. FORM OF BUSINESS

a. Applicant is a(an): ☐ Individual ☒ Corporation ☐ Partnership ☐ Other: _____

b. Date established: 1961

c. Description of operations: Automotive Dealership

d. Total number of employees: 2500

e. Attach a list of all subsidiaries, affiliated companies or entities owned by the Applicant and include a description of (1) the nature of operations of each such subsidiary, affiliated company or entity, (2) its relationship to the Applicant and (3) the percentage of ownership by the Applicant.

3. REVENUES

	<u>Current</u> Fiscal Year ending 12 / 24 (current projected)	<u>Last</u> Fiscal Year ending 12 / 23	<u>Two</u> Fiscal Years ago ending 12 / 22
Total gross revenues:	\$ [REDACTED]	\$ [REDACTED]	\$ [REDACTED]

4. RECORDS

a. Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form? ☒ Yes ☐ No

If "Yes", provide the approximate number of unique records:

Paper records: [REDACTED] Electronic records: [REDACTED]

*Private or sensitive information includes any information or data that can be used to uniquely identify a person, including, but not limited to, social security numbers or other government identification numbers, payment card information, drivers' license numbers, financial account numbers, personal identification numbers (PINs), usernames, passwords, healthcare records and email addresses.

b. Do you collect, store, host, process, control, use or share any biometric information or data, such as fingerprints, voiceprints, facial, hand, iris or retinal scans, DNA, or any other biological, physical or behavioral characteristics that can be used to uniquely identify a person? ☐ Yes ☒ No

If "Yes", have you reviewed your policies relating to the collection, storage and destruction of such information or data with a qualified attorney and confirmed compliance with applicable federal, state, local and foreign laws? ☐ Yes ☐ No

c. Do you process, store or handle credit card transactions? ☒ Yes ☐ No

If "Yes", are you PCI-DSS Compliant? ☒ Yes ☐ No

5. IT DEPARTMENT

This section must be completed by the individual within the Applicant's organization who is responsible for network security. As used in this section only, "you" refers only to such individual.

a. Within the Applicant's organization, who is responsible for network security?

Name: Conrad Sarnessar

Title: Security Admin

Phone: [REDACTED]

Email address: conrads@findlayauto.com

IT Security Designation(s): Security Officer Conrad

b. The Applicant's network security is: ☐ Outsourced; provide the name of your network security provider:

☒ Managed internally/in-house

c. If the Applicant's network security is outsourced, are you the main contact for the network security provider named in question b. above? ☐ Yes ☐ No

If "No", provide the name and email address for the main contact: Conrad Samessar conrads@indiatayauto.com

d. How many IT personnel are on your team? 7

e. How many dedicated IT security personnel are on your team? 2

By signing below, you confirm that you have reviewed all questions in Sections 6 through 8 of this application regarding the Applicant's security controls, and, to the best of your knowledge, all answers are complete and accurate. Additionally, you consent to receiving direct communications from the Insurer and/or its representatives regarding potentially urgent security issues identified in relation to the Applicant's organization.

Print/Type Name: John Steffy

Signature: [Redacted Signature]

6. EMAIL SECURITY CONTROLS

If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section.

a. Do you tag external emails to alert employees that the message originated from outside the organization? ☒ Yes ☐ No

b. Do you pre-screen emails for potentially malicious attachments and links? ☒ Yes ☐ No

If "Yes", complete the following:

(1) Select your email security provider: Microsoft Defender

If "Other", provide the name of your email security provider: _____

(2) Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if they are malicious prior to delivery to the end-user? ☒ Yes ☐ No

c. Have you implemented any of the following to protect against phishing messages? (check all that apply):

☒ Sender Policy Framework (SPF)

☒ DomainKeys Identified Mail (DKIM)

☒ Domain-based Message Authentication, Reporting & Conformance (DMARC)

☐ None of the above

d. Can your users access email through a web application or a non-corporate device? ☒ Yes ☐ No

If "Yes", do you enforce Multi-Factor Authentication (MFA)? ☒ Yes ☐ No

e. Do you use Office 365 in your organization? ☒ Yes ☐ No

If "Yes", do you use the Office 365 Advanced Threat Protection add-on? ☒ Yes ☐ No

ADDITIONAL COMMENTS (Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)

7. INTERNAL SECURITY CONTROLS

If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section.

a. Do you use a cloud provider to store data or host applications? ☒ Yes ☐ No

If "Yes", provide the name of the cloud provider: CDK Global

If you use more than one cloud provider to store data, specify the cloud provider storing the largest quantity of sensitive customer and/or employee records (e.g., including medical records, personal health information, social security numbers, bank account details and credit card numbers) for you.

b. Do you use MFA to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud)? ☒ Yes ☐ No

c. Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? ☐ Yes ☒ No

If "No", are the following compensating controls in place:

(1) Segregation of servers that store sensitive and confidential information? ☒ Yes ☐ No

(2) Access control with role-based assignments? ☒ Yes ☐ No

d. Do you allow remote access to your network? ☒ Yes ☐ No

If "Yes", do you use MFA to secure all remote access to your network, including any remote desktop protocol (RDP) connections? ☒ Yes ☐ No

If MFA is used, complete the following:

(1) Select your MFA provider: Duo

If "Other", provide the name of your MFA provider: Duo & Okta on some Apps

(2) Select your MFA type: Push-based authentication

If "Other", describe your MFA type: Duo is push based

(3) Does your MFA configuration ensure that the compromise of a single device will only compromise a single authenticator? ☒ Yes ☐ No

e. Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise? ☒ Yes ☐ No

If "Yes", select your NGAV provider: Cisco

If "Other", provide the name of your NGAV provider: _____

f. Do you use an endpoint detection and response (EDR) tool that includes centralized monitoring and logging of all endpoint activity across your enterprise? ☒ Yes ☐ No

If "Yes", complete the following:

(1) Select your EDR provider: Cisco AMP

If "Other", provide the name of your EDR provider: _____

(2) Do you enforce application whitelisting/blacklisting? ☒ Yes ☐ No

(3) Is EDR deployed on 100% of endpoints? ☒ Yes ☐ No

If "No", please use the Additional Comments section to outline which assets do not have EDR, and whether any mitigating safeguards are in place for such assets.

(4) Can users access the network with their own device ("Bring Your Own Device")? ☐ Yes ☒ No

If "Yes", is EDR required to be installed on these devices? ☐ Yes ☐ No

g. Do you use MFA to protect all local and remote access to privileged user accounts? ☒ Yes ☐ No

If "Yes", select your MFA type: Push-based authentication

If "Other", describe your MFA type: _____

h. Do you manage privileged accounts using privileged account management software (PAM) (e.g., CyberArk, BeyondTrust, etc.)? ☐ Yes ☒ No

If "Yes", complete the following:

(1) Provide the name of your software provider: All Privileged Accounts are IT Zero Trust

(2) Is access protected by MFA? ☒ Yes ☐ No

i. Do you actively monitor all administrator access for unusual behavior patterns? ☒ Yes ☐ No

If "Yes", provide the name of your monitoring tool: Palo Alto internal

j. Do you roll out a hardened baseline configuration across servers, laptops, desktops and managed mobile devices? ☒ Yes ☐ No

k. Do you record and track all software and hardware assets deployed across your organization? ☒ Yes ☐ No

If "Yes", provide the name of the tool used for this purpose (if any): _____

l. Do non-IT users have local administration rights on their laptop / desktop? ☐ Yes ☒ No

m. How frequently do you install critical and high severity patches across your enterprise?

☐ 1-3 days ☒ 4-7 days ☐ 8-30 days ☐ One month or longer

n. Do you have any end of life or end of support software? ☐ Yes ☒ No

If "Yes", is it segregated from the rest of your network? ☐ Yes ☐ No

o. Do you use a protective DNS service (PDNS) (e.g. ZScaler, Quad9, OpenDNS or the public sector PDNS to block access to known malicious websites? ☒ Yes ☐ No

If "Yes", provide the name of your DNS provider: Cisco Umbrella

p. Do you use endpoint application isolation and containment technology on all endpoints? ☒ Yes ☐ No

If "Yes", select your provider: Other

If "Other", provide the name of your provider: AMP

q. Can users run Microsoft Office Macro enabled documents on their system by default? ☐ Yes ☒ No

r. Do you implement PowerShell best practices as outlined in the Environment Recommendations by Microsoft? ☒ Yes ☐ No

s. Do you utilize a Security Information and Event Management system (SIEM)? ☒ Yes ☐ No

t. Do you utilize a Security Operations Center (SOC)?

☒ Yes ☐ No

If "Yes", complete the following:

(1) Is your SOC monitored 24 hours a day, 7 days a week?

☒ Yes ☐ No

(2) Your SOC is: ☒ Outsourced; provide the name of your provider: Port 53

☐ Managed internally/in-house

u. Do you use a vulnerability management tool?

☒ Yes ☐ No

If "Yes", complete the following:

(1) Select your provider: Other

If "Other", provide the name of your provider: Kace

(2) What is your patching cadence?

☐ 1-3 days ☒ 4-7 days ☐ 8-30 days ☐ 1 month or longer

ADDITIONAL COMMENTS (Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)

8. BACKUP AND RECOVERY POLICIES

If the answer to the question in this section is "No", please provide additional details in the "Additional Comments" section.

Do you use a data backup solution?

☒ Yes ☐ No

If "Yes":

a. Which best describes your data backup solution?

☐ Backups are kept locally but separate from your network (offline/air-gapped backup solution).

☐ Backups are kept in a dedicated cloud backup service.

☐ You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive).

☒ Other (describe your data backup solution): Our own Cloud in Switch Data Center

b. Check all that apply:

☒ Your backups are encrypted.

☐ You have immutable backups.

☒ Your backups are secured with different access credentials from other administrator credentials.

☒ You utilize MFA for both internal and external access to your backups.

☒ You have tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months.

☒ You are able to test the integrity of backups prior to restoration to ensure that they are free of malware.

c. How frequently are backups run? ☒ Daily ☐ Weekly ☐ Monthly

d. Estimated amount of time it will take to restore essential functions using backups in the event of a widespread malware or ransomware attack within your network?

☒ 0-24 hours ☐ 1-3 days ☐ 4-6 days ☐ 1 week or longer

ADDITIONAL COMMENTS (Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)

9. PHISHING CONTROLS

a. Do any of the following employees at your company complete social engineering training:

(1) Employees with financial or accounting responsibilities?

☒ Yes ☐ No

(2) Employees without financial or accounting responsibilities?

☒ Yes ☐ No

If "Yes" to question 9.a.(1) or 9.a.(2) above, does your social engineering training include phishing simulation?

☐ Yes ☒ No

b. Does your organization send and/or receive wire transfers?

☐ Yes ☒ No

If "Yes", does your wire transfer authorization process include the following:

(1) A wire request documentation form?

☐ Yes ☐ No

(2) A protocol for obtaining proper written authorization for wire transfers?

☐ Yes ☐ No

- (3) A separation of authority protocol? ☐ Yes ☐ No
- (4) A protocol for confirming all payment or funds transfer instructions/requests from a new vendor, client or customer via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the payment or funds transfer instruction/request was received? ☐ Yes ☐ No
- (5) A protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information or mailing addresses) via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the change request was received? ☐ Yes ☐ No

10. LOSS HISTORY

If the answer to any question in 10.a. through 10.c. below is "Yes", please complete a Claim Supplemental Form for each claim, allegation or incident.

- a. In the past 3 years, has the Applicant or any other person or organization proposed for this insurance:
- (1) Received any complaints or written demands or been a subject in litigation involving matters of privacy injury, breach of private information, network security, defamation, content infringement, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks or the ability of third parties to rely on the Applicant's network? ☐ Yes ☒ No
- (2) Been the subject of any government action, investigation or other proceedings regarding any alleged violation of privacy law or regulation? ☐ Yes ☒ No
- (3) Notified customers, clients or any third party of any security breach or privacy breach? ☐ Yes ☒ No
- (4) Received any cyber extortion demand or threat? ☐ Yes ☒ No
- (5) Sustained any unscheduled network outage or interruption for any reason? ☐ Yes ☒ No
- (6) Sustained any property damage or business interruption losses as a result of a cyber-attack? ☐ Yes ☒ No
- (7) Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud? ☐ Yes ☒ No
- b. Do you or any other person or organization proposed for this insurance have knowledge of any security breach, privacy breach, privacy-related event or incident or allegations of breach of privacy that may give rise to a claim? ☐ Yes ☒ No
- c. In the past 3 years, has any service provider with access to the Applicant's network or computer system(s) sustained an unscheduled network outage or interruption lasting longer than 4 hours? ☐ Yes ☒ No
- If "Yes", did the Applicant experience an interruption in business as a result of such outage or interruption? ☐ Yes ☐ No

NOTICE TO APPLICANT

The insurance for which you are applying will not respond to incidents about which any person proposed for coverage had knowledge prior to the effective date of the policy nor will coverage apply to any claim or circumstance identified or that should have been identified in questions 10.a. through 10.c of this application.

NOTICE TO NEW YORK APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE CONTAINING ANY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME.

The Applicant hereby acknowledges that he/she/it is aware that the limit of liability shall be reduced, and may be completely exhausted, by claim expenses and, in such event, the Insurer shall not be liable for claim expenses or any judgment or settlement that exceed the limit of liability.

I HEREBY DECLARE that, after inquiry, the above statements and particulars are true and I have not suppressed or misstated any material fact, and that I agree that this application shall be the basis of the contract with the Underwriters.

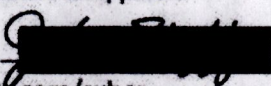
CERTIFICATION AND SIGNATURE

The Applicant has read the foregoing and understands that completion of this application does not bind the Underwriter or the Broker to provide coverage. It is agreed, however, that this application is complete and correct to the best of the Applicant's knowledge and belief, and that all particulars which may have a bearing upon acceptability as a NetGuard® Plus Cyber Liability Insurance risk have been revealed.

It is understood that this application shall form the basis of the contract should the Underwriter approve coverage, and should the Applicant be satisfied with the Underwriter's quotation. It is further agreed that, if in the time between submission of this application and the requested date for coverage to be effective, the Applicant becomes aware of any information which would change the answers furnished in response to any question of this application, such information shall be revealed immediately in writing to the Underwriter.

This application shall be deemed attached to and form a part of the Policy should coverage be bound.

Must be signed by an officer of the company.

Print or Type Applicant's Name John Steffy	Title of Applicant CIO
Signature of Applicant 	Date Signed by Applicant 04/30/2024

tmhcc.com/cyber

EXHIBIT 2

JUNE 7, 2024 EMAIL FROM RONDA MINER

From: Ronda Miner
To: Michael Armstrong (CA); Cassandra Fnu; Morgan Deese (CA)
Cc: Alice Li; Sales Distribution
Subject: RE: Findlay Management Group, Inc / TMHCC Primary Quote
Date: Friday, June 7, 2024 12:45:55 PM
Attachments: HCC REVISED \$5M Primary.pdf

Good morning Michael,

Happy Friday! Please bind coverage effective **6/1/2024** per the attached quote.

We will coordinate the signed required binding documents as soon as possible.

Thank you for your help on this account!

Kindly,

Ronda Miner | Senior Account Analyst
CA License Number 4307015

Thaxton & Associates
CA License Number 0C69104
11338 Moorpark St. Studio City CA 91602
t 818.508.6500 ext 248 | f 818.655.1287

From: Michael Armstrong (CA) <MArmstrong@crcgroup.com>
Sent: Wednesday, June 5, 2024 9:28 AM
To: Michael Armstrong (CA) <marmstrong@crcgroup.com>; Cassandra Fnu
<Cassandra@thaxtonassociates.com>; Morgan Deese (CA) <MDeese@crcgroup.com>
Cc: Alice Li <alicali@thaxtonassociates.com>; Sales Distribution <sales@thaxtonassociates.com>
Subject: RE: Findlay Management Group, Inc / TMHCC Primary Quote

Revised primary TMHCC quote @ \$70K premium! We were able to negotiate down \$10K.

Working on confirmation with excess markets on their revised pricing. Updates to come!

Best,

Michael Armstrong MLIS, RPLU
CA License # 4199983
Broker | Executive Professional Practice Group
LA ExecPro Team << [Click Here!](#)

Cell: (949) 290 - 3605
E-mail: MArmstrong@crcgroup.com

CRC Group | CA License # 0778135
crcgroup.com
333 South Grand Avenue, # 1570, Los Angeles, CA 90071

EXHIBIT 3

NETGUARD® PLUS CYBER LIABILITY INSURANCE QUESTIONNAIRE

DocuSign Envelope ID: D1A07850-0CD5-4A24-9719-6B8ACBB90015

TOKIO MARINE
HCC

NetGuard® Plus Cyber Liability Insurance

APPLICATION

THIS IS AN APPLICATION FOR A CLAIMS MADE AND REPORTED POLICY. THIS APPLICATION IS NOT A BINDER.

This application for NetGuard® Plus Cyber Liability Insurance is intended to be used for the preliminary evaluation of a submission. When completed in its entirety, this application will enable the Underwriter to decide whether or not to authorize the binding of insurance. Please type or print clearly and answer all questions. If space is insufficient to answer any question fully, attach a separate sheet. Complete all required supplemental forms/applications. "You" and "Your", as used in this application, means the Applicant unless noted otherwise below.

Please refer to the attached Cyber Glossary for an explanation of the cyber security terms that appear in bold face type.

1. GENERAL INFORMATION

Name of Applicant: Findlay Management

Street Address: 310 N. Gibson Road

City, State, Zip: Henderson

Phone: 702 558 8888

Website: findlayauto.com

Fax:

2. FORM OF BUSINESSa. Applicant is a(an): ☐ Individual ☒ Corporation ☐ Partnership ☐ Other: _____

b. Date established: 1961

c. Description of operations: Automotive Dealership

d. Total number of employees: 2500

e. Attach a list of all subsidiaries, affiliated companies or entities owned by the Applicant and include a description of (1) the nature of operations of each such subsidiary, affiliated company or entity, (2) its relationship to the Applicant and (3) the percentage of ownership by the Applicant.

3. REVENUES

	<u>Current</u> Fiscal Year ending 12 / 24 (current projected)	<u>Last</u> Fiscal Year ending 12 / 23	<u>Two</u> Fiscal Years ago ending 12 / 22
Total gross revenues:	\$ [REDACTED]	\$ [REDACTED]	\$ [REDACTED]

4. RECORDS

a. Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form? ☒ Yes ☐ No

If "Yes", provide the approximate number of unique records:

Paper records: [REDACTED] Electronic records: [REDACTED]

*Private or sensitive information includes any information or data that can be used to uniquely identify a person, including, but not limited to, social security numbers or other government identification numbers, payment card information, drivers' license numbers, financial account numbers, personal identification numbers (PINs), usernames, passwords, healthcare records and email addresses.

b. Do you collect, store, host, process, control, use or share any biometric information or data, such as fingerprints, voiceprints, facial, hand, iris or retinal scans, DNA, or any other biological, physical or behavioral characteristics that can be used to uniquely identify a person? ☐ Yes ☒ No

If "Yes", have you reviewed your policies relating to the collection, storage and destruction of such information or data with a qualified attorney and confirmed compliance with applicable federal, state, local and foreign laws? ☐ Yes ☐ No

c. Do you process, store or handle credit card transactions? ☒ Yes ☐ No

If "Yes", are you PCI-DSS Compliant? ☒ Yes ☐ No

5. IT DEPARTMENT

This section must be completed by the individual within the Applicant's organization who is responsible for network security. As used in this section only, "you" refers only to such individual.

a. Within the Applicant's organization, who is responsible for network security?

Name: Conrad Samessar

Title: Security Admin

Phone: [REDACTED]


Email address: conrads@findlayauto.com

IT Security Designation(s): Security Officer Conrad

DocuSign Envelope ID: D1A07850-0CD5-4A24-9719-6B8ACBB90015

b. The Applicant's network security is: ☐ Outsourced; provide the name of your network security provider:☒ Managed Internally/in-housec. If the Applicant's network security is outsourced, are you the main contact for the network security provider named in question b. above? ☐ Yes ☐ NoIf "No", provide the name and email address for the main contact: Conrad Samassar conrad@findlayauto.comd. How many IT personnel are on your team? 7e. How many dedicated IT security personnel are on your team? 2

By signing below, you confirm that you have reviewed all questions in Sections 6 through 8 of this application regarding the Applicant's security controls, and, to the best of your knowledge, all answers are complete and accurate. Additionally, you consent to receiving direct communications from the Insurer and/or its representatives regarding potentially urgent security issues identified in relation to the Applicant's organization.

Print/Type Name: John SteffySignature: **6. EMAIL SECURITY CONTROLS**

If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section.

a. Do you tag external emails to alert employees that the message originated from outside the organization? ☒ Yes ☐ Nob. Do you pre-screen emails for potentially malicious attachments and links? ☒ Yes ☐ No

If "Yes", complete the following:

(1) Select your email security provider: Microsoft Defender

If "Other", provide the name of your email security provider: _____

(2) Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if they are malicious prior to delivery to the end-user? ☒ Yes ☐ No

c. Have you implemented any of the following to protect against phishing messages? (check all that apply):

☒ Sender Policy Framework (SPF)☒ DomainKeys Identified Mail (DKIM)☒ Domain-based Message Authentication, Reporting & Conformance (DMARC)☐ None of the aboved. Can your users access email through a web application or a non-corporate device? ☒ Yes ☐ NoIf "Yes", do you enforce Multi-Factor Authentication (MFA)? ☒ Yes ☐ Noe. Do you use Office 365 in your organization? ☒ Yes ☐ NoIf "Yes", do you use the Office 365 Advanced Threat Protection add-on? ☒ Yes ☐ No

ADDITIONAL COMMENTS (Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)

7. INTERNAL SECURITY CONTROLS

If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section.

a. Do you use a cloud provider to store data or host applications? ☒ Yes ☐ NoIf "Yes", provide the name of the cloud provider: CDK Global

If you use more than one cloud provider to store data, specify the cloud provider storing the largest quantity of sensitive customer and/or employee records (e.g., including medical records, personal health information, social security numbers, bank account details and credit card numbers) for you.

b. Do you use MFA to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud)? ☒ Yes ☐ Noc. Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? ☐ Yes ☒ No

If "No", are the following compensating controls in place:

(1) Segregation of servers that store sensitive and confidential information? ☒ Yes ☐ No(2) Access control with role-based assignments? ☒ Yes ☐ Nod. Do you allow remote access to your network? ☒ Yes ☐ NoIf "Yes", do you use MFA to secure all remote access to your network, including any remote desktop protocol (RDP) connections? ☒ Yes ☐ No

If MFA is used, complete the following:

tmhcc.com/cyber

NGP-NBA (11.2021)

DocuSign Envelope ID: D1A07850-0CD5-4A24-9719-6B8ACBB90015

(1) Select your MFA provider: Duo
If "Other", provide the name of your MFA provider: Duo & Okta on some Apps

(2) Select your MFA type: Push-based authentication
If "Other", describe your MFA type: Duo is push based

(3) Does your MFA configuration ensure that the compromise of a single device will only compromise a single authenticator? ☒ Yes ☐ No

e. Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise? ☒ Yes ☐ No
If "Yes", select your NGAV provider: Cisco
If "Other", provide the name of your NGAV provider: _____

f. Do you use an endpoint detection and response (EDR) tool that includes centralized monitoring and logging of all endpoint activity across your enterprise? ☒ Yes ☐ No
If "Yes", complete the following:
(1) Select your EDR provider: Cisco AMP
If "Other", provide the name of your EDR provider: _____
(2) Do you enforce application whitelisting/blacklisting? ☒ Yes ☐ No
(3) Is EDR deployed on 100% of endpoints? ☒ Yes ☐ No
If "No", please use the Additional Comments section to outline which assets do not have EDR, and whether any mitigating safeguards are in place for such assets.
(4) Can users access the network with their own device ("Bring Your Own Device")? ☐ Yes ☒ No
If "Yes", is EDR required to be installed on these devices? ☐ Yes ☐ No

g. Do you use MFA to protect all local and remote access to privileged user accounts? ☒ Yes ☐ No
If "Yes", select your MFA type: Push-based authentication
If "Other", describe your MFA type: _____

h. Do you manage privileged accounts using privileged account management software (PAM) (e.g., CyberArk, BeyondTrust, etc.)? ☐ Yes ☒ No
If "Yes", complete the following:
(1) Provide the name of your software provider: All Privileged Accounts are IT Zero Trust
(2) Is access protected by MFA? ☒ Yes ☐ No

i. Do you actively monitor all administrator access for unusual behavior patterns? ☒ Yes ☐ No
If "Yes", provide the name of your monitoring tool: Palo Alto Internal

j. Do you roll out a hardened baseline configuration across servers, laptops, desktops and managed mobile devices? ☒ Yes ☐ No

k. Do you record and track all software and hardware assets deployed across your organization? ☒ Yes ☐ No
If "Yes", provide the name of the tool used for this purpose (if any): _____

l. Do non-IT users have local administration rights on their laptop / desktop? ☐ Yes ☒ No

m. How frequently do you install critical and high severity patches across your enterprise?
☐ 1-3 days ☒ 4-7 days ☐ 8-30 days ☐ One month or longer

n. Do you have any end of life or end of support software? ☐ Yes ☒ No
If "Yes", is it segregated from the rest of your network? ☐ Yes ☐ No

o. Do you use a protective DNS service (PDNS) (e.g. ZScaler, Quad9, OpenDNS or the public sector PDNS to block access to known malicious websites? ☒ Yes ☐ No
If "Yes", provide the name of your DNS provider: Cisco Umbrella

p. Do you use endpoint application isolation and containment technology on all endpoints? ☒ Yes ☐ No
If "Yes", select your provider: Other
If "Other", provide the name of your provider: AMP

q. Can users run Microsoft Office Macro enabled documents on their system by default? ☐ Yes ☒ No

r. Do you implement PowerShell best practices as outlined in the Environment Recommendations by Microsoft? ☒ Yes ☐ No

s. Do you utilize a Security Information and Event Management system (SIEM)? ☒ Yes ☐ No

DocuSign Envelope ID: D1A07850-0CD5-4A24-9719-6B8ACBB90015

t. Do you utilize a Security Operations Center (SOC)?

☒ Yes ☐ No

If "Yes", complete the following:

(1) Is your SOC monitored 24 hours a day, 7 days a week?

☒ Yes ☐ No(2) Your SOC is: ☒ Outsourced; provide the name of your provider: Port 53☐ Managed internally/in-house

u. Do you use a vulnerability management tool?

☒ Yes ☐ No

If "Yes", complete the following:

(1) Select your provider: OtherIf "Other", provide the name of your provider: Kase

(2) What is your patching cadence?

☐ 1-3 days ☒ 4-7 days ☐ 8-30 days ☐ 1 month or longer**ADDITIONAL COMMENTS** (Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)**8. BACKUP AND RECOVERY POLICIES**

If the answer to the question in this section is "No", please provide additional details in the "Additional Comments" section.

Do you use a data backup solution?

☒ Yes ☐ No

If "Yes":

a. Which best describes your data backup solution?

☐ Backups are kept locally but separate from your network (offline/air-gapped backup solution).☐ Backups are kept in a dedicated cloud backup service.☐ You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive).☒ Other (describe your data backup solution): Our own Cloud in Switch Data Center

b. Check all that apply:

☒ Your backups are encrypted.☐ You have immutable backups.☒ Your backups are secured with different access credentials from other administrator credentials.☒ You utilize MFA for both internal and external access to your backups.☒ You have tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months.☒ You are able to test the integrity of backups prior to restoration to ensure that they are free of malware.c. How frequently are backups run? ☒ Daily ☐ Weekly ☐ Monthly

d. Estimated amount of time it will take to restore essential functions using backups in the event of a widespread malware or ransomware attack within your network?

☒ 0-24 hours ☐ 1-3 days ☐ 4-6 days ☐ 1 week or longer**ADDITIONAL COMMENTS** (Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)**9. PHISHING CONTROLS**

a. Do any of the following employees at your company complete social engineering training:

(1) Employees with financial or accounting responsibilities?☒ Yes ☐ No(2) Employees without financial or accounting responsibilities?☒ Yes ☐ No

If "Yes" to question 9.a.(1) or 9.a.(2) above, does your social engineering training include phishing simulation?

☐ Yes ☒ No

b. Does your organization send and/or receive wire transfers?

☐ Yes ☒ No

If "Yes", does your wire transfer authorization process include the following:

(1) A wire request documentation form?

☐ Yes ☐ No

(2) A protocol for obtaining proper written authorization for wire transfers?

☐ Yes ☐ No

DocuSign Envelope ID: D1A07850-0CD5-4A24-9719-6B8ACBB90015

- (3) A separation of authority protocol? ☐ Yes ☐ No
- (4) A protocol for confirming all payment or funds transfer instructions/requests from a new vendor, client or customer via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the payment or funds transfer instruction/request was received? ☐ Yes ☐ No
- (5) A protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information or mailing addresses) via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the change request was received? ☐ Yes ☐ No

10. LOSS HISTORY

If the answer to any question in 10.a. through 10.c. below is "Yes", please complete a Claim Supplemental Form for each claim, allegation or incident.

- a. In the past 3 years, has the Applicant or any other person or organization proposed for this insurance:
- (1) Received any complaints or written demands or been a subject in litigation involving matters of privacy injury, breach of private information, network security, defamation, content infringement, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks or the ability of third parties to rely on the Applicant's network? ☐ Yes ☒ No
- (2) Been the subject of any government action, investigation or other proceedings regarding any alleged violation of privacy law or regulation? ☐ Yes ☒ No
- (3) Notified customers, clients or any third party of any security breach or privacy breach? ☐ Yes ☒ No
- (4) Received any cyber extortion demand or threat? ☐ Yes ☒ No
- (5) Sustained any unscheduled network outage or interruption for any reason? ☐ Yes ☒ No
- (6) Sustained any property damage or business interruption losses as a result of a cyber-attack? ☐ Yes ☒ No
- (7) Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud? ☐ Yes ☒ No
- b. Do you or any other person or organization proposed for this insurance have knowledge of any security breach, privacy breach, privacy-related event or incident or allegations of breach of privacy that may give rise to a claim? ☐ Yes ☒ No
- c. In the past 3 years, has any service provider with access to the Applicant's network or computer system(s) sustained an unscheduled network outage or interruption lasting longer than 4 hours? ☐ Yes ☒ No
- If "Yes", did the Applicant experience an interruption in business as a result of such outage or interruption? ☐ Yes ☐ No

NOTICE TO APPLICANT

The insurance for which you are applying will not respond to incidents about which any person proposed for coverage had knowledge prior to the effective date of the policy nor will coverage apply to any claim or circumstance identified or that should have been identified in questions 10.a. through 10.c of this application.

NOTICE TO NEW YORK APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE CONTAINING ANY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME.

The Applicant hereby acknowledges that he/she/it is aware that the limit of liability shall be reduced, and may be completely exhausted, by claim expenses and, in such event, the insurer shall not be liable for claim expenses or any judgment or settlement that exceed the limit of liability.

I HEREBY DECLARE that, after inquiry, the above statements and particulars are true and I have not suppressed or misstated any material fact, and that I agree that this application shall be the basis of the contract with the Underwriters.

CERTIFICATION AND SIGNATURE

The Applicant has read the foregoing and understands that completion of this application does not bind the Underwriter or the Broker to provide coverage. It is agreed, however, that this application is complete and correct to the best of the Applicant's knowledge and belief, and that all particulars which may have a bearing upon acceptability as a NetGuard® Plus Cyber Liability Insurance risk have been revealed.

It is understood that this application shall form the basis of the contract should the Underwriter approve coverage, and should the Applicant be satisfied with the Underwriter's quotation. It is further agreed that, if in the time between submission of this application and the requested date for coverage to be effective, the Applicant becomes aware of any information which would change the answers furnished in response to any question of this application, such information shall be revealed immediately in writing to the Underwriter.

This application shall be deemed attached to and form a part of the Policy should coverage be bound.

Must be signed by an officer of the company.

Print or Type Applicant's Name
Tyler Corder

Title of Applicant
CFO

Signature of Applicant

Date Signed by Applicant
6/1/2024

tmhcc.com/cyber

NGP-NBA (11.2021)

Page 5 of 5

(5) Sus
(6) Sus
(7) Sus

b. Do you
breach,
to a clai

c. In the p
sustaine
If "Yes",

NOTICE TO APPL
The insurance fo
knowledge prior
have been identifi

**NOTICE TO NEW
COMPANY OR C
CONCEALS FOR
FRAUDULENT IN**
The Applicant he
exhausted, by cla
that exceed the li

I HEREBY DECL
any material fact,

CERTIFICATION
The Applicant has
provide coverage
and that all partic
revealed.

It is understood th
be satisfied with th
date for coverage
to be checked, and application becomes aware of any information which would change the answers furni
to any question of this application, such information shall be revealed immediately in writing to the Underwriter.
This application shall be deemed attached to and form a part of the Policy should coverage be bound.

Must be signed by an officer of the company.

Print or Type Applicant's Name Tyler Corder	Title of Applicant CFO
Signature of Applicant Tyler Corder	Date Signed by Applicant 6/1/2024

tmhcc.com/cyber

Signature is VALID, signed by DocuSign, Inc.
<enterprisesupport@docuSign.com>
Signing Time: 2024/06/07 11:30:10 -07'00'
Source of Trust obtained from Adobe Approved Trust List (AATL).
Reason: Digitally verifiable PDF exported from www.docuSign.com

Validity Summary
The document has not been modified since this signature was applied.
The certifier has specified that Form Fill-in, Signing and Commenting are allowed for this document. No other changes are permitted.
The signer's identity is valid.
Signing time is from the clock on the signer's computer.
Signature was validated as of the signing time
2024/06/07 11:30:10 -07'00'

Signer Info
The path from the signer's certificate to an issuer's certificate was successfully built.
The signer's certificate is valid and has not been revoked.

[Show Signer's Certificate...](#)

[Advanced Properties...](#) [Validate Signature](#) [Close](#)

[Export...](#)

NOTIFICATION
Applic
de co
that a
aled.
unders
atisfie
for co
y que
applic
be si
or Ty

The selected certificate path is valid.

The path validation and revocation checks were done as of the signing time:
2024/06/07 11:30:10 -07'00'
Validation Model: Shell